Electronic Version
Stylesheet Version v1.1.1

Claims

[c1] 1. A method for detecting intrusion in a host via a monitoring daemon operating in conjunction with a configuration file defining data entities to be monitored, said method as implemented in said host comprising the steps of:
a. monitoring said data entities via comparing a locally stored copy of a digital signature associated with each data entity against a corresponding digital signature stored in a first remote database; and
b. upon identifying a mismatch in compared digital signatures, issuing an instruction to record an entry in a log file located in a second remote database, said entry identifying a possible intrusion in said host.

[c2] 2. A method for detecting intrusion in a host via a monitoring daemon operating in conjunction with a configuration file defining data entities to be monitored, as per claim 1, wherein said host communicates with said first and second remote databases via one or more network interfaces and, subsequent to step (b), said method further comprises the step of issuing a command to bring down said one or more network interfaces to isolate said

host.

[c3] 3. A method for detecting intrusion in a host via a monitoring daemon operating in conjunction with a configuration file defining data entities to be monitored, as per claim 1, wherein, subsequent to step (b), said method further comprises the step of issuing a command to an operating system of host to bring said host to a single user state.

[c4] 4. A method for detecting intrusion in a host via a monitoring daemon operating in conjunction with a configuration file defining data entities to be monitored, as per claim 1, wherein said first remote database and said second remote database are located on a single server or a plurality of servers belonging to a local area network.

[c5] 5. A method for detecting intrusion in a host via a monitoring daemon operating in conjunction with a configuration file defining data entities to be monitored, as per claim 1, wherein communications between said host and first remote database are encrypted.

[c6] 6. A method for detecting intrusion in a host via a monitoring daemon operating in conjunction with a configuration file defining data entities to be monitored, as per claim 1, wherein communications between said host and

second remote database are encrypted.

[c7] 7. A method for detecting intrusion in a host via a monitoring daemon operating in conjunction with a configuration file defining data entities to be monitored, as per claim 1, wherein said digital signature is an MD5 signature and said first remote database is an MD5 database.

[c8] 8. A method for detecting intrusion in a host via a monitoring daemon operating in conjunction with a configuration file defining data entities to be monitored, as per claim 1, wherein said second remote database is a SYSLOG database.

[c9] 9. A method for detecting intrusion in a host via a monitoring daemon operating in conjunction with a configuration file defining data entities to be monitored, as per claim 1, wherein said data entities are any of the following: system files, configuration files, or directories.

[c10] 10. A system to detect intrusion comprising:
a. a host running a monitoring daemon working in conjunction with a configuration file, said configuration file identifying files and directories to be monitored in said host and said host communicating with external networks via one or more network interfaces, said monitoring daemon dynamically monitoring said files and direc-

tories identified by said configuration file by comparing a locally stored digital signature corresponding to each file or directory against a remotely stored corresponding digital signature;

b. a digital signature database remote from said host storing said digital signatures associated with files and directories identified by said configuration file; and

c. a log database remote from said host recording entries corresponding to mismatches between a digital signature stored in said host and a corresponding digital signature in said digital signature database.

[c11] 11. A system to detect intrusion as per claim 10, wherein said first remote database and said second remote database are located on a single server or a plurality of servers belonging to a local area network.

[c12] 12. A system to detect intrusion as per claim 10, wherein communications between said host and said digital signature database are encrypted.

[c13] 13. A system to detect intrusion as per claim 10, wherein communications between said host and log database are encrypted.

[c14] 14. A system to detect intrusion as per claim 10, wherein said digital signature is an MD5 signature and said first

remote database is an MD5 database.

[c15] 15. An article of manufacture comprising a computer usable medium having computer readable program code embed therein to detect intrusion in a host via a monitoring daemon operating in conjunction with a configuration file defining data entities to be monitored, said medium comprising:

a. computer readable program code monitoring said data entities via comparing a locally stored copy of a digital signature associated with each data entity against a corresponding digital signature stored in a first remote database; and

b. upon identifying a mismatch in compared digital signatures, computer readable program code issuing an instruction to record an entry in a log file located in a second remote database, said entry identifying a possible intrusion in said host.

[c16] 16. An article of manufacture as per claim 15, wherein said host communicates with said first and second remote databases via one or more network interfaces and said medium further comprises computer readable program code issuing a command to bring down said one or more network interfaces to isolate said host.

[c17] 17. An article of manufacture, as per claim 15, wherein

said method further comprises the step of issuing a command to an operating system of host to bring said host to a single user state.

[c18] 18. An intrusion detection and isolation method implemented using a monitoring daemon in a host, said host having one or more network interfaces to communicate over one or more networks, said method comprising the steps of:

a. reading a configuration file to identify data entities to be monitored on a host;

b. for each data entity to be monitored, extracting a digital signature from said host;

c. for each data entity to be monitored, querying a remote digital signature database via said one or more network interfaces and requesting a digital signature corresponding to said digital signature extracted from said host;

d. for each data entity to be monitored, receiving said corresponding digital signature from said remote digital signature database;

e. matching digital signature received from said remote digital signature database with digital signature extracted at said host;

f. upon identifying a mismatch, transmitting an instruction to a remote log database via said one or more net-

work interfaces, said instruction executed in said remote log database to record an entry in a log file indicating a possible intrusion in said host; and

g. performing any one of, or a combination of, the following steps:

(i) issuing a command to bring down said one or more network interfaces to isolate said host; or

(ii) issuing a command to an operating system of host to bring said host to a single user state.

[c19] 19. An intrusion detection and isolation method implemented using a monitoring daemon in a host, as per claim 18, wherein said digital signature database and said log database are located on a single server or a plurality of servers belonging to a local area network.

[c20] 20. An intrusion detection and isolation method implemented using a monitoring daemon in a host, as per claim 18, wherein communications between said host and digital signature database are encrypted.

[c21] 21. An intrusion detection and isolation method implemented using a monitoring daemon in a host, as per claim 18, wherein communications between said host and log database are encrypted.

[c22] 22. An intrusion detection and isolation method imple-

mented using a monitoring daemon in a host, as per claim 18, wherein said digital signature database is an MD5 database.

[c23] 23. An intrusion detection and isolation method implemented using a monitoring daemon in a host, as per claim 18, wherein said log database is a SYSLOG database.

[c24] 24. An intrusion detection and isolation method implemented using a monitoring daemon in a host, as per claim 18, wherein said data entities are any of the following: system files, configuration files, or directories.